L Number	Hits	Search Text	DB	Time stamp
-	1	20020112181.pn.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 12:35
-	39	(multi$1level adj secure$2) and proxy	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 12:37
-	1	diode adj server	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 12:37
-	1819	thin adj client	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 12:38
-	2	((multi$1level adj secure$2) and proxy) and (thin adj client)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 14:21
-	855	(second adj network) and proxy	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 14:40
-	1	(remote adj session) with viewer	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 14:25
-	6	(remote adj session) and ((second adj network) and proxy)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/03 09:30
-	150	(intermediate adj network) and proxy	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 14:41
-	136	remote adj session	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 14:42
-	3	((intermediate adj network) and proxy) and (remote adj session)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 14:42
-	27287	diode with direction$	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 16:06
-	508	(diode with direction$) and security	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/02 16:07
-	20	(diode with direction$) same security	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/03 13:17
-	33	(remote adj session) and proxy	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/03 09:30
-	1	5940591.pn.	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/03 12:07
-	9671	(diode) and security	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/03 13:18

-	944	(diode) same security	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/03 13:18
-	3	(information adj diode) same security	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/04 09:16
-	6013	central$ and (proxy or (remote adj session))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/04 09:17
-	858	central$ same (proxy or (remote adj session))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/04 09:18
-	395	central$ with (proxy or (remote adj session))	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/04 09:18
-	308	central$ with (proxy or (remote adj session)) and (rout$3 or switch$)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/04 10:03
-	68	central$ with (proxy or (remote adj session)) same (rout$3 or switch$)	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/04 09:23
-	42	(central$ with (proxy or (remote adj session)) same (rout$3 or switch$)) and security	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/04 10:03
-	197	(central$ and (proxy or (remote adj session))) and diode	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/04 09:52
-	21	(central$ same (proxy or (remote adj session))) and diode	USPAT; US-PGPUB; EPO; JPO; IBM_TDB	2004/06/04 09:52

Multilevel Security in the Departme of the Defen

Multilevel Security in the Department Of Defense: The Basics

This document was edited for network access by the Department Of Defense Multilevel Security Program.

This document is releasable to the public.

1 March 1995

PREFACE

The Basics provides an explanation of multilevel security (MLS) technology and its operational capabilities for program managers, action officers, and others who are faced with the task of determining if and how MLS technology could be beneficial in their information systems. It contains a set of MLS Dos and Don'ts that can guide readers in their pursuit of MLS capabilities.

This document also introduces the Department of Defense (DoD) MLS Program. In addition to the program's mission and goals, this document describes the primary MLS capabilities that the program is developing and deploying.

This document consists of four sections and an appendix. Section 1

introduces MLS. Section 2 discusses the DoD MLS Program. Section 3 discusses the concepts associated with MLS and introduces the basic MLS technologies that can provide MLS capabilities. Section 4 offers guidance for greater success in achieving MLS capabilities. The appendix presents a short list of acronyms.

TABLE OF CONTENTS

INTRODUCTION

A significant challenge exists throughout the Department of Defense (DoD) in getting mission-critical and time-sensitive information into the hands of people who need it. All too often, the information resides in information systems that do not provide access to persons outside the immediate community of interest.

The DoD relies on information systems to support the missions of nearly every organization. In most cases today, information is protected at the highest classification level of the data in the system, the system-high level. Thus, the information is not readily accessible by persons not cleared to the system-high level, even though the information being sought may be of a lower classification level and thereby releasable to the requester. Operating information systems in this manner often results in the over-classification of data, over-clearing of personnel, and system redundancies and inefficiencies. This situation commonly exists throughout the DoD. What is needed is a means by which the actual security level of the information can be maintained and information can be appropriately protected, processed, and distributed. Users also need timely access to the data and the various processing and communications resources that they require to accomplish their jobs.

The security constraints imposed by the system-high mode of operation on DoD information systems often result in less than effective operations. For example, tape, disk, and paper copy output are often manually reviewed, downgraded, and transferred through time-consuming and labor-intensive procedures among systems operating at different security levels. This method of data transfer is often inefficient and ineffective. It can also result in the inefficient use of personnel and resources, a condition that challenges the current downsizing requirements facing many government organizations.

In addition, staff members need to access and fuse data and other resources currently available on several systems to perform their duties. Each system generally has its own interface (e.g., via a specific set of terminals or workstations), requiring multiple terminals that take valuable space in command centers, offices, and computer rooms. Also, significant time and effort are needed to manually fuse data from different sources.

The maintenance of redundant data bases is another unfavorable condition that results from using separate systems for each security level. Often a separate data base must be created and maintained for each security level processed. The use of these multiple data bases presents several operational problems. First, it fragments

information. A collection of information regarding a specific event may be split across multiple systems of different security levels. Incomplete or misleading information may result unless pertinent data can be obtained from all related systems. Second, information of a lower classification may be unnecessarily upgraded in the higher level systems, resulting in its over-classification and consequent limited access. As a result, duplication and multiple classifications of the same information occurs. Third, the maintenance of multiple data bases is staff intensive and depletes other system resources. Because the data may change continually, updating data bases often results in inconsistent views of the current information across different levels. The constantly changing nature of the data, combined with human updating, often results in outdated information at one or more of the security levels.

Another difficulty when multiple systems operate at different security levels is the inability to share the computer and communication system infrastructures, such as cabling, network components, printers, workstations, and hosts. If sharing these resources were possible, equipment, operations, and maintenance costs would decrease.

Multilevel security, or MLS, is a capability that allows information with different sensitivities (i.e., classification and compartments) to be simultaneously stored and processed in an information system with users having different security clearances, authorizations, and needs to know, while preventing users from accessing information for which they are not cleared, do not have authorization, or do not have the need to know. MLS capabilities often can help overcome the operational constraints imposed by system-high operations and can foster more effective operations. For example, systems once separated by an airgap or connected only by a sneaker net may be electronically interconnected by an MLS guard, allowing the data transferred to be current rather than merely historical in value.

Additionally, staff members who once had to use several different terminals for day-to-day operations may now access the systems they need from an MLS workstation, allowing a single, secure interface to the systems they use.

MLS guards and MLS workstations can be used to bridge security boundaries between existing single-level systems. Ideally, information systems themselves will become MLS systems to provide more integrated multilevel capabilities for users. MLS hosts, MLS networks, and MLS data base management systems (DBMS) can provide common data processing and data transfer

platforms to serve as the foundation for MLS systems. A larger community that once may have been segregated for security reasons may be electronically integrated to more effectively and efficiently execute its collective mission.

MLS technology is real and in use today. As the technology evolves with the computer and communications industry, its capabilities will provide the DoD with increasing mission effectiveness. MLS is a significant enabling technology for command, control, communications, and intelligence systems because it enhances the availability of information while maintaining security. For this reason, it is important to understand what capabilities MLS can provide and to integrate those capabilities into DoD information systems now and into the next century.

THE DoD MLS PROGRAM

The DoD MLS Program provides a focal point within the DoD to promote the development and implementation of MLS solutions for information systems. The mission of the program is to expedite the fielding of MLS capabilities in the DoD. The goal of the program is to develop, acquire, and deploy solutions and technologies that will allow the DoD to meet operational requirements for MLS in its automated information systems. The program accomplishes this goal through the following activities:

*Planning, coordinating, reviewing, and assessing MLS efforts throughout the DoD to provide synergy and to reduce duplication of effort

*Developing and assessing MLS technology for widespread application through approved architectures

*Providing engineering assistance to the DoD to expedite the transfer of MLS capabilities from testbeds to operational systems

The program is managed by the Defense Information Systems Agency/Joint Interoperability and Engineering Organization/Center for Information Systems Security, with the sponsorship and oversight from the Assistant Secretary of Defense for Command, Control, Communications, and Intelligence and the Joint Staff. The National Security Agency (NSA) is the security technical coordinator for the program, and the Defense Intelligence Agency is the intelligence coordinator. This combination brings the resources and capabilities of the key DoD information systems security

(INFOSEC) organizations together to meet the challenges faced when developing and deploying MLS capabilities.

The DoD MLS Program provides the following products, services, and capabilities to DoD organizations.

Technology Surveys and Assessments. Technical and operational assessments of the MLS marketplace and its utility.

Surveys and Assessments Available Today

*Trusted Workstation Survey and Assessments

*Xerox Encryption Unit Assessment

*Loral Multinet Gateway MLS-100 Assessment

*Secure Network Demonstration

*SecureWare MaxSix Assessment

Surveys and Assessments Scheduled for Fiscal Year (FY) 94

*Trusted Host and Workstation Survey

*Trusted DBMS Survey

*Trusted Network Survey

*MLS Guard Survey

MLS Solution Sets. A set of government off-the-shelf and commercial off-the-shelf near-term solutions to common requirements for MLS (discussed in greater detail in Section 3.4):

*Standard Guards

*Operations (OPS)/Intelligence (INTEL) Interfaces

*MLS Workstations.

System Security Profiles. A repository of security-related assessments of MLS products and configurations to streamline the certification of MLS solutions. These profiles draw on previously tested, assessed, and evaluated configurations to assist in the system certification and accreditation process.

MLS Assistance. A wide range of MLS technical and programmatic support to DoD organizations:

*MLS requirements analysis, solution identification, security policy definition, and concept of operations development

*Certification and accreditation planning, analysis, and testing

*Project review and other consultation (e.g., MLS help desk).

MLS Deployments. Installation and integration of MLS solution sets at the Unified Commands and other high-priority commands.

MLS Demonstration and Assessment Center. A facility dedicated to investigating the application of MLS products and technology to fulfill DoD operational requirements. The MLS Demonstration and Assessment Center:

*Assesses existing emerging MLS products and technology

*Advances new approaches to MLS

*Provides a neutral demonstration environment for MLS vendors

*Maintains a DoD-wide perspective on MLS solutions.

The DoD MLS Program provides solutions to resolve interoperability problems between existing system-high environments. The program offers expertise, technologies, and capabilities to help DoD organizations solve similar problems.

THE MLS ENVIRONMENT

This section defines characteristics and components of the MLS environment. It explains the operational requirements for MLS technology and the problems the DoD faces with its current systems. It explores potential MLS solutions, emphasizing the need to implement an incremental approach that builds toward a full MLS capability.

Multilevel security allows information systems to provide capabilities that augment its existing single-level data processing

and data communications services. Data of multiple security levels are processed and transferred by the system, which also separates the different security levels and controls access to the data. Applications are provided, much in the same way that they exist today, so that users can access, process, modify, store, and transfer data. For example, office automation (e.g., word processing, electronic filing, spreadsheets), data base management, data fusion, modeling and simulation, briefing and display, command and control, and decision support applications are needed as much in an MLS system as they are in existing single-level systems. Some applications process only one level of data at a time, such as when a user edits a document with a word processing tool. In this case, the data in the document are treated as if they were a single level, the classification of the document itself. More complex applications could be provided that treat individual data elements at their actual levels. For example, a word processor could enforce paragraph and page labels, or an MLS data base could bring together data elements of different security levels to allow an analyst a multilevel view of the information.

With the concept in mind that MLS systems can provide capabilities similar to existing, single-level applications, but for data of multiple security levels, one can understand the multilevel mode of operation and the basic building blocks that form MLS systems.

3.1 MULTILEVEL MODE OF OPERATION

In the DoD, a system's security operations are characterized according to minimum user clearances and the maximum security levels of data either processed or transferred by the systems. According to these characteristics, the DoD defines the following four modes of operation:

Dedicated System high Partitioned (or compartmented) Multilevel.

Restrictions on the user clearance levels, formal authorization requirements (i.e., for access to special access programs, compartmented information, and other close-hold data), need-to-know requirements, and the range of sensitive information permitted on the system are inherent in each of these security modes. The following chart illustrates the characteristics of each mode of operation.

As one progresses from the dedicated and system high modes to the partitioned and multilevel modes, there is a shift from providing security using physical controls, administrative procedures, and personnel security to using computer security, communications security, and trusted system techniques. Each mode of operation requires the use of security features to provide the required level of protection. The dedicated mode (where all users possess clearance levels greater than or equal to the highest level of data to be processed, all users have formal authorization, and all users have the need to know for the data) has the fewest security requirements, followed by system high, then partitioned and multilevel, which require the most security protection because there is an increasing risk that insufficiently cleared persons may gain access to data for which they lack authorization.

When a system operates in the multilevel mode, it allows data of two or more security levels to be processed simultaneously when not all users have the clearance, formal authorization, or need to know for all data handled by the system. The system is able to separate and protect the data according to these restrictions.

To amplify the definition, an MLS system might process both Secret and Top Secret collateral data and have some users whose maximum clearance is Secret and others whose maximum clearance is Top Secret. Another MLS system might have all its users cleared at the Top Secret level, but have the ability to release information classified as Secret to a network consisting of only Secret users and systems. Still another system might process both Secret and Unclassified information and have some users with no clearance. In each of these instances, the system must implement mechanisms to provide assurance that the system's security policy is strictly enforced. In these examples, the policy allows access to the data by only those users who are appropriately cleared and authorized (e.g., having formal access approval) and who have an official need to know for the data.

A related mode of operation is the partitioned mode, also known as compartmented mode. Although similar concepts and solutions are involved for compartmented mode operations as are for the multilevel mode, there is also a key difference. In the compartmented mode, all users have clearances for all the data processed but may not have authorizations for all the data; whereas for multilevel mode, some users may not even be cleared for the highest level. Because the compartmented mode is often envisioned for the intelligence community, all such users would have Top Secret security clearances and often authorizations for one or more,

but possibly not all, compartments in the system.

DoD security regulations state that systems must receive approval to operate (in a particular mode) from their accreditation authorities. This approval is also known as an accreditation and indicates that the cognizant authorities have accepted the evidence that the system has sufficient features and assurance to allow operations while maintaining an acceptable level of risk. Only certain trusted technology provides the features and assurances required by the accreditation authorities for multilevel mode operations. The next section focuses on that technology.

3.2 TRUSTED COMPUTER SYSTEM EVALUATION CRITERIA

The trusted computer system evaluation criteria defined in DoD 5200.28-STD, also known as the Orange Book because of its bright orange cover, classifies systems into four broad hierarchical divisions of increasing security protection. The criteria provide the basis for evaluating the effectiveness of the security controls built into the products used in information systems.

The criteria were developed to provide users a measure with which to assess the degree of trust that can be placed in computer systems for the secure processing of classified or other sensitive information. In general, secure systems will control, through the use of specific security features, access to data such that only properly authorized individuals, or processes operating on their behalf, will have access to read, write, delete, or execute data.

The criteria are divided into four divisions -- D, C, B, and A -- ordered in a hierarchical manner with the highest division (A) reserved for systems providing the most comprehensive security. Each division represents a major increase in the overall confidence, or trust, that one can place in the system. Successive levels of trust build upon and incorporate the criteria of the previous lower level of trust.

Within Divisions C and B there are a number of subdivisions known as classes. The classes are also ordered in a hierarchical manner with systems representative of Divisions C and B characterized by the set of computer security mechanisms that they possess. For Division C, so called discretionary protection is provided, whereby users can grant or deny access by other users

and groups of users to the system resources that the users control. For Division B, mandatory protection is provided that, in conjunction with the discretionary protection, institutionalizes hierarchical access controls that can be used to separate and protect data of different security levels. Division A also provides the mandatory protection features.

Systems representative of the higher classes in Division B and Division A derive their security attributes more from their design and implementation structure than merely security features or functionality. Increased assurance that the required features are operative, correct, and tamperproof under all circumstances is gained through progressively more rigorous design, implementation, and analysis during the development process. Division A requires formal (e.g., mathematical) design and verification techniques to provide increased assurances over Division B.

Four major sets of criteria apply to each class. The first three sets represent features necessary to satisfy broad control objectives of security policy, accountability, and assurance. The fourth set, documentation, defines the type of written information such as user guides, manuals, and the test and design documentation required for each class.

MLS capabilities are associated with Division B and A products. In these classes, security mechanisms are in place to ensure that only authorized users with clearances and need to know can access the data. Assurances to increase confidence that the mechanisms are functioning securely increase in the higher classes; B2, B3, and A1 class components offer progressively more assurance than do B1 class components. The following table summarizes the key characteristics of each class. The security requirements increase as the division and class increase. The dashed line shows division where MLS capabilities are introduced into the criteria (i.e., in divisions A and B). The reader should explore DoD 5200.28-STD for more information on the levels of trust.

Division Class Title Key Charact.

D N/A Minimal Protection None (a rating given to products that do not meet all of the criteria of another class)

C C1 Discretionary Security Protection Discretionary Access Control, User Authentication

C2 Controlled Access Protection All of C1, plus Audit Trails, Individual Passwords, Object Reuse

---

B B1 Labeled Security Protection All of C2, plus Labels, Mandatory Access Control, Informal Security Policy Model

B2 Structured Protection All of B1, plus Structured Trusted Computing Base (TCB), Trusted Path, Covert Channel Analysis, Penetration Resistance, Configurati Management

B3 Security Domains All of B2, plus Formal Security Policy Model, Minimal and Tamperproof TCB, Trusted Recovery, Substantial Documentation

A A1 Verified Design All of B3, plus Formal Specification, Formal Design Verification, Trusted Distributn

The NSA has also published interpretations of the trusted systems criteria that apply to other components such as networks, data base management systems, and other computer subsystems. The levels of trust defined in DoD 5200.28-STD, however, are not directly applicable to systems, but solely to components in systems. Products that the NSA has evaluated and that meet these criteria are recorded in the Evaluated Products List in NSA's Information Systems Security Products and Services Catalogue, which is updated and published quarterly.

Not all MLS products are formally evaluated and placed on the Evaluated Products List. However, most MLS products are built according to the DoD 5200.28-STD criteria or an interpretation, and some measure of assurance may be derived for those products as well.

3.3 MLS CONCEPT OF OPERATIONS

The introduction of MLS capabilities in an existing organization will result not only in changes in effectiveness and security of operations, but also in the manner business is conducted using information systems. MLS affects business processes in many ways, from providing users with multilevel views of data that they

previously accessed separately, to maintaining electronic sensitivity labels (e.g., classification markings, handling restrictions) on data that are processed and transferred by the system. Although the specific effects MLS technology has on the manner in which users work will depend on numerous factors (e.g., the specific technology used, the specific application software applied, and the business processes themselves), the general impact of MLS on operations is summarized as follows:

Sensitivity Labels. All data must be properly labeled as to their classification and other handling restrictions if an MLS system is to properly control access to the data. In system-high operations, a user may create data (e.g., create a message on a word processor) that have security levels equal to or less than the system-high level, but all data must be protected at the system-high level until they are reliably reviewed for their actual classification and removed from the system. In many MLS systems, users make decisions at login time as to the security level at which they want to operate, knowing that files created during the session will be labeled according to their session security level. In MLS systems with multilevel windowing capabilities, the user must also make conscious decisions as to the security level of data at the time of the data's creation, rather than afterwards*****. This type of decision needs to be made often, for example, when composing an electronic mail message, creating a document, entering data into a data base, and creating graphs and charts.

In the partitioned or compartmented mode, information labels are companions to sensitivity labels. Where sensitivity labels indicate the overall classification of a data container, such as a file or a window on the computer screen, information labels represent the actual security level of the data within the container. Access control decisions (e.g., whether a user is allowed to access a file) are made based on sensitivity labels; information labels are referenced by users to determine the actual classification of the data viewed.

Multilevel Processing. MLS systems offer users the ability to process and transfer data of more than one security level while maintaining control of the data according to their sensitivity. Users could, for example, edit a Secret document, then edit an Unclassified document as part of a continuous session. In other cases, users may access multilevel data bases and have access to the information contained in them according to their security level. For example, an uncleared user may have access to only the Unclassified portions of a data base, while a Secret-cleared user may have access to Secret portions in addition to the Unclassified portions. Users would be able to share more synchronous and consistent information when multilevel data bases allow currently

segregated collections of data to be securely combined. In general, multilevel processing capabilities will allow access to multiple levels of data from a single work position and use of a common set of data processing tools (e.g., word processors, decision support tools, data base management systems).

Planners considering MLS capabilities must remember that MLS does not eliminate the need for physical and personnel security for computers, networks, and other components that will process or transfer classified data. The components still contain the data in their memories and disks, and the data could be compromised if adequate physical security was not maintained.

3.4 POTENTIAL MLS SOLUTIONS

Achieving an MLS system solution to meet operational needs involves determining how to integrate the different stand-alone legacy information systems and networks into integrated and interoperable information systems. The resulting information systems should allow authorized users to simultaneously access multiple levels of classified data and to securely gain access to classified information originally maintained by the separate stand-alone information systems. Achieving this end is not the result of an instantaneous action. Attainment of an integrated MLS capability is predicated on the completion of the following:

Developing system capabilities that allow systems, at differing classification levels, to interact Developing and acquiring MLS technology such as hosts, workstations, data base management systems, and networks Developing expertise and techniques for securely integrating the different components into MLS systems that meet operational requirements.

All the major components--the hosts, workstations, data base management systems, and networks--work together to separate and protect data of different security levels (e.g., classifications, compartments) from users of differing clearance levels. One noteworthy aspect of an MLS architecture is that not all components need to be trusted. Therefore, a typical system needing MLS capabilities might have only a few trusted components with the remainder being single level. This combination allows a more optimal balance between security and functionality to be achieved.

Successfully reaching such an MLS solution requires a strategy. The strategy for achieving an MLS capability requires an incremental approach that reduces development risks. Shown below is a recommended implementation strategy for integrating MLS capabilities to meet operational requirements.

Each increment introduces components that provide additional MLS capabilities. Together these components will construct MLS systems that allow for the processing of data of multiple classifications while providing the assurance that users of differing clearance levels only have access to data for which they possess the clearance, authorization, and need to know. Discussions of each of the component technologies follow.

3.4.1 MLS Hosts

An MLS host is the primary multiuser component of an MLS system. MLS hosts are the basic building blocks of MLS systems, and as such perform a variety of data processing and data transfer services, from functioning as file servers, mail servers, and print servers to serving as the platforms for system applications such as command and control systems, data base management systems, and decision support systems. MLS hosts are compositions of trusted operating systems running on any variety of hardware platforms, such as microcomputers, minicomputers, and mainframe computers. Several products have been evaluated by the NSA that can serve as MLS hosts and are currently available.

The operational value of MLS hosts derives from some high-assurance products available to serve MLS systems. High-assurance MLS hosts could be used to allow wide ranges of classified data and cleared users to access a system (e.g., up to Top Secret data with some users uncleared). Some products that could serve as MLS hosts, however, are not necessarily high assurance (e.g., some are B1 and B2 class products).

3.4.2 MLS Guards

MLS guards control the flow of information across security boundaries. They are often the initial step toward MLS because they can be relatively simple to achieve and can provide some of the interconnectivity required to bridge across the security boundaries

of existing systems operating at different security levels. Several types of guards exist. They might or might not involve human review of the data flow and might support data flow in one or both directions. Guards generally do not allow full-capability usage of a system on one side of the guard by users from the other side, but rather support only limited types of data transfers. As previously illustrated, MLS guards partially break through the wall of security constraints that restrict the flow of data among systems operating at different security levels.

MLS guards can be implemented as one-way filters (e.g., allowing low-to-high or high-to-low data flow only) or as bidirectional filters for data traffic between systems. Low-to-high guards are available today and can be deployed with relatively low development risk. Low-to-high guards allow data flow from a lower classified system to a higher classified system without data flow in the other direction. This capability is useful when users of high systems need data from lower systems in electronic form in a timely manner. One-way, low-to-high guards may need to prevent the transfer of malicious code (e.g., viruses), of forged identifiers, and of intentional network flooding attempts that could result in denial of service conditions on the high side. Some of these guards have been successfully operational in various DoD organizations for several years. However, the most effective use of a guard is bidirectional, because a two-way flow of data allows more robust communication protocols and provides more reliable data transfer. For example, a one-way guard provides no receipt or acknowledgment for data transfers because such a receipt would violate the security policy rule governing the one-way flow of data.

The rules for high-to-low data flow are often more complex than those for low-to-high data flow, because the guards are required to enforce complicated and sometimes dynamic security policy (e.g., classification rules). Guards can be implemented to check whether the data bound for the low system is classified at the low system's security level. This check could be executed in several ways, such as by ensuring that the data are of a specific content or format, ensuring that the data do not contain any defined classified code words or phrases (e.g., "dirty words"), or even ensuring that the data have a specific sensitivity label. If the checks pass, the guard downgrades the data and passes them to the low system.

Guards can also be implemented to actually change the data (e.g., sanitization or downgrading). The guard could accept data from the high system and apply specific processes to the data to reduce their security levels to that of the low system before it downgrades the information and passes it to the low system. A human may be called into the process at any point necessary to review specific data and

make decisions when the computer is unable. For example, free-form text found in electronic mail is beyond the ability of computers to check for classification. Humans may be needed to review such data for classification before they are released to the low system.

The ideal guard would be capable of correctly reviewing or sanitizing any form and content of data without human intervention. We are, however, a long way from that ideal guard. The technology that shapes the artificial intelligence necessary to review any given format, declare it safe, and assure the user that it was executed properly, is not currently available.

The DoD MLS Program is developing and deploying guards to partially meet common requirements for MLS in the near term. The Standard WWMCCS Guard provides a means for DoD organizations to extract Secret and less classified data from the Top Secret Worldwide Military Command and Control System (WWMCCS), which operates in the system-high mode, and to make that data available to users on Secret command and control systems. The guard reviews all data transfers according to the established classification rules to verify that the data passed are not classified Top Secret. It handles a wide range of high-to-low and low-to-high data transfers, including Time Phased Force and Deployment Data, Status of Readiness and Training System data, electronic mail, and teleconference messages. The guard has been certified and accredited by the Joint Staff for use with WWMCCS.

The DoD MLS Program is also developing and deploying another standard guard to meet common operational requirements in the near term--the Standard Mail Guard. The guard allows users of existing Secret and Unclassified communities to securely exchange Unclassified electronic mail. The guard relies on users to review messages before they send them to verify that only Unclassified data are exchanged between the Secret community and the Unclassified community.

3.4.3 MLS Workstations

A workstation is a user terminal with its own processing and storage capabilities. It can be linked to a local area network that can provide a number of services (e.g. electronic mail, word processing, computation, and remote file access). MLS workstations are workstations that can separate and protect data of different security levels. Compartmented mode workstations (CMW) are the

predominate type of MLS workstation and specifically meet the requirements set forth by the Defense Intelligence Agency to support multilevel and compartmented mode operations of intelligence analysts. CMWs provide a multilevel, multiwindowing capability that permits users to have windows of different security levels open simultaneously on their computer screens. This trusted multiwindowing capability is a critical element in making MLS workstations operationally effective.

The initial goal of an MLS workstation is to allow a user to access systems operating at different security levels simultaneously from a single position. The concept involves the MLS workstation with two network connections, one for the high side, another for the low side. An MLS workstation provides improved capability over a guard because it supports full capability usage of both high and low existing systems from one workstation. An MLS workstation should not affect the existing systems themselves but should provide a user enhanced access to the systems. Several current development efforts with MLS workstation technology meet these operational requirements.

In MLS workstations, the trusted multiwindowing capability can be used to support interaction with multiple systems or application software. The trusted workstations allow users to access systems and application software at different classification levels simultaneously and transfer data between security levels (if the user has the appropriate authority). For example, information can be transferred from the Secret system to the Top Secret system. Information from the Top Secret system can be sanitized or downgraded, if necessary, and sent to the Secret system after review. The users can also alternate working with both systems through the multiple windows.

The DoD MLS Program is developing and deploying MLS workstations not only to bridge different security levels in a command and control infrastructure, but also to enhance the data communications between intelligence organizations and the commands that they support. Using MLS workstations and other network security techniques, the program developed the OPS/INTEL Interface to facilitate more interaction between intelligence analysts and the command staff. The OPS/INTEL Interface provides capabilities to intelligence analysts to pull data from various intelligence resources, review and, if needed, sanitize the data, and electronically pass the data to collateral systems for further access and processing. The OPS/INTEL Interface also provides a means for requests for intelligence to be sent by command staff and electronically received by the intelligence analysts.

3.4.4 MLS Networks

A multilevel network is the logical next step to follow the installation of multilevel workstations. An MLS network can provide secure data communication services among components in information systems. MLS networks can interconnect single-level and multilevel components on a shared network infrastructure by providing sensitivity labels and network security services for the data transferred between systems. MLS networks do not need to have any MLS hosts or workstations on them to make them effective solutions; the MLS networks may simply allow single-level hosts and workstations of different security levels to share a common infrastructure.

MLS network components are used for both local area networks and wide area networks, which are composed of numerous elements, such as cabling, terminal servers, bridges, routers, and gateways. In an MLS network, several of these elements are trusted to enforce the security policy for the network.

3.4.5 MLS Data Base Management Systems

MLS DBMSs provide the management, storage, and retrieval of multiple levels of related data, allowing users of different security levels to have access to a shared set of data according to their individual authorizations. For example, a DBMS server is accessible to both the Secret and Top Secret users. Top Secret cleared users have access to read the entire data base. Secret cleared users are restricted to reading and writing within the confines of the Secret portion of the data base. Security mechanisms are in place to enforce this policy, including sensitivity labels for various data base constructs like tables, views, and records. MLS DBMSs manage and control user queries according to the security levels of the data and the user clearances. They can eliminate duplication of information on separate systems, resulting in more timely, consistent, and accurate data. MLS DBMSs will serve as the foundation for many applications in MLS systems.

3.4.6 MLS Systems

The ultimate goal of MLS is not simply to interconnect existing single-level systems operating at different security levels, or even to allow users to perform office automation functions at multiple security levels (albeit maintaining separation of data of different levels). Rather, the goal is to foster a truly multilevel environment, whereby a user can process data of multiple levels in a more integral manner.

Consider, for example, a multilevel document preparation system that allows a user to label individual paragraphs and section headings with their classifications. This system would accurately label pages according to the maximum classification of the paragraphs on the pages, and allow cutting and pasting among documents while still maintaining sensitivity labels and enforcing security rules so that more classified paragraphs are not included in less classified reports.

Another example involves a multilevel data base to direct and monitor military transportation, including points and times of embarkment and destination, transit route, crew information, and cargo information. This data base could be used to direct and track missions that are both unclassified and classified. However, because some information about the classified missions needs to be visible at the unclassified level, the MLS DBMS supporting this application would allow classified users to enter and retrieve both classified and unclassified data about the missions. By providing cover stories so that some information is available at the unclassified level, uncleared persons could coordinate for the arrival of aircraft requiring specific off-loading equipment. The unclassified users of this system could have, then, limited visibility into the various missions.

The goal MLS system combines the MLS hosts, workstations, DBMSs, networks, and other components with multilevel applications to comprise an integrated multilevel environment rather than only a lashing together of multiple single-level elements. These MLS systems could be applied to command and control, office automation, data fusion, decision support, and other uses throughout the DoD.

MLS DOs AND DON'Ts

Current MLS technology is evolving. Even so, the available technology is widely applicable to DoD programs, and emerging

MLS technology will have an even greater impact. There are several concepts to keep in mind and adages to apply when considering MLS technology and capabilities.

Do: Integrate INFOSEC engineering into the system life cycle.

Don't: Think that security can be retrofitted into systems .

Security planning and other security-related activities must be a total life cycle activity. The success of an MLS system development or acquisition requires effective security planning beginning with the earliest phases of the life cycle. To succeed in implementing MLS technology, security must be viewed as an integral functional requirement throughout the system acquisition. MLS provides capabilities to meet operational requirements while overcoming some of the traditional constraints that security imposes on information systems. This recognition promotes the effective incorporation of security-related activities throughout the entire system acquisition life cycle. Retrofitting security features and assurances into a system is inefficient and often more costly than it would have been to originally include security into the design, implementation, and operations.

Do: Rethink your operational concept to understand how MLS will meet and enhance your operational requirements.

Don't: Buy a solution and then look for a requirement.

Understanding at the earliest possible time the operational requirements of the system and how the system is intended to be used will allow for the effective analysis and selection of solutions. Many areas need to be examined in defining the requirements. For example, the concept of operations addresses the following questions:

What mission is the system to support? What is the function of the system? What are the initial and future connections? What is the data sensitivity range? Who are the intended users and what are their roles? What clearances and authorizations do the users have? How can MLS be used to automate the users' jobs? What is the flow of information among users and systems?

A firm understanding of the operational requirements helps to create an effective concept of operations for the system. When the operational requirements are understood, MLS capabilities can be selected to meet both the operational and security requirements. This type of approach considers, we have these requirements, therefore which security solution can satisfy them?, instead of an approach that questions, that vendor has an MLS widget, now how can we use it?

Do: Identify and involve your accreditors early in the MLS project.

Don't: Risk the project with your interpretation of ambiguous security regulations and policy.

The accreditor for a system, sometimes known as its Designated Approving Authority (DAA), is responsible through policy and directive for the security of that system. Therefore, the accreditor should be identified and involved in the system acquisition process from its initiation. The participation of accreditation authorities in the system definition activities will provide them insight into the rationale for the security approach chosen. This is especially important in an MLS environment where accreditors have few tools or methods with which to assess the security solutions implemented. No amount of academic rationalization regarding risk indexes and levels of trust will be of use for a program manager if the accreditor is uncomfortable with the proposed solution. The accreditor should be involved with or made aware of design, implementation, and operational proposals and decisions throughout the system life cycle. Many systems have multiple accreditation authorities because the systems have connections with other systems and networks. Any such interconnections should be identified early in the system concept and requirements stages.

Do: Approach MLS incrementally.

Don't: Pick unrealistic near-term goals.

Program managers should follow workable and proven strategies for achieving MLS capabilities. For example, the implementation strategy being undertaken by the DoD MLS Program begins with the deployment of MLS guards and workstations at the interfaces

between systems operating at different security levels in the near term, followed with the integration of MLS components to create MLS systems in the long term. The DoD MLS Program recommends this approach for both new system developments and existing system enhancements. The near-term time frame is considered as the current fiscal year through the next. The long term time frame is thereafter. Users with especially critical operational requirements for MLS might choose to pursue more aggressive approaches that entail higher costs and greater development risks. As time progresses, the foundation MLS technology should be able to provide increasing functionality and increasing assurances (e.g., levels of trust).

The DoD MLS Program has demonstrated the usefulness of prototyping MLS capabilities before trying to build operational capabilities. Prototyping can help validate system security requirements, demonstrate feasibility, reduce uncertainty and risk, and increase the chances of user acceptance of a new concept of operations. Prototyping provides the opportunity to develop a set of realistic functional requirements, something useful with an MLS system. The opportunity to refine and validate security requirements should not be overlooked.

Whatever the approach, be sure to choose near-term goals that can be met, and build incrementally, so that MLS capabilities can be integrated as they become available over the years.

Do: Design and develop MLS capabilities using existing technology.

Don't: Base the success of your project on the hype of the latest vendor marketing call.

The National Security Agency evaluates commercial products and certain government technology against the trusted computer system evaluation criteria in DoD 5200.28-STD or one of its interpretations for networks, DBMSs, or computer subsystems. NSA's evaluation investigates not only a product's security features, but also the assurances in the product's design and implementation that the security is correct and complete. Program managers and system integrators can take advantage of NSA's efforts in the design and implementation of MLS capabilities that use these trusted products.

The benefits of using evaluated products are typically evident in the certification process, when a system undergoes its own security assessment to ensure that it satisfies its security requirements and

will allow operations with an acceptable level of risk. An evaluated product has already undergone elements of that assessment itself, and its use in the system may require less effort to facilitate the system certification. For example, one can have confidence that a product having successfully completed an NSA evaluation meets a certain set of the security requirements placed on it as part of an MLS system. However, a similar unevaluated product, providing a similar set of functional and security services, would bring with it no such confidences and would require that the program manager assess those security services more comprehensively in the system certification process.

Many vendors, in an effort to advertise their products, make claims that the products are designed to meet the criteria of a certain DoD 5200.28-STD class. Such claims should only be accepted when backed by a certificate from the NSA or a listing in the Evaluated Products List.

To allow multilevel processing in the range set of Unclassified through Secret, Secret through Top Secret, or Top Secret through Top Secret with compartments, current DoD and NSA guidance for determining an appropriate level of trust requires a level of protection equal to the B2 class. However, most of the MLS workstation platforms are evaluated at the B1 class. This results in a workstation that can provide much of the needed functionality, but not the higher level of assurance associated with a B2 class product. This limited selection of higher assurance products sometimes leads to the decision to use lower assurance products (e.g., B1 class) to meet important operational needs. The result is multilevel functionality without the complementary assurances or trust.*******

There are other system requirements to consider in addition to the security requirements, and a program manager must make trade-offs when selecting technology to meet the total set of requirements on a system. When MLS is an operational requirement, program managers should consider first the set of evaluated products to satisfy the requirement. If the set of available, evaluated products does not meet the needs, products in evaluation or derived from evaluated products (e.g., such as from using a different hardware platform or a more recent version of the operating system) should be considered. Other products with claims to provide MLS capabilities but that are not evaluated or in evaluation should be investigated only after evaluated technology has been exhausted.

Do: Consider information technology standards for MLS solutions.

Don't: Accept proprietary solutions without good reason.

The computer and communications industry has adopted various standards that promote interoperability among networked computer systems, operating systems, and application software. For example, the following standards are significant in the development and integration of information systems:

Portable Operating System Interface for Computer Environments (POSIX) for operating system interfaces Government Open Systems Interconnection Profile (GOSIP) for network protocols Structured Query Language (SQL) for DBMSs X-Windows for windowing applications.

Many MLS products use these standards for the definitions of their interfaces. By adhering to these and other industry standards in the development of MLS systems, the systems are provided a more flexible basis for enhancements and for changes in the system platforms (e.g., porting the application software to another standards-compliant operating system or DBMS) when the selection of products is as limited as it is for MLS technology. This flexibility is crucial to mitigate development risks.

Do: Coordinate with the DoD MLS Program.

Don't: Ignore the lessons learned and experiences from other MLS projects.

The DoD MLS Program not only manages and sponsors numerous MLS projects throughout the DoD, but it also monitors dozens of other projects in the DoD and with other government agencies. The DoD MLS Program maintains a selection of lesson learned documents, technology assessments, and other information to help program managers guide the development and operations of systems with operational requirements for MLS. In addition to the published materials, the DoD MLS Program provides other consultation with DoD and other organizations to help them meet their MLS needs.

Appendix -- Acronyms

Acronym Meaning

CMW Compartmented Mode Workstation

COTS Commercial Off-the-Shelf

DBMS Data Base Management System

DAA Designated Approving Authority

DoD Department of Defense

FY Fiscal Year

GOSIP Government Open Systems Interconnection Profile

INFOSEC Information Systems Security

MLS Multilevel Security

NSA National Security Agency

OPS/INTEL Operations/Intelligence

POSIX Portable Operating System Interface for Computer Environments

SQL Structured Query Language

TCB Trusted Computing Base

WWMCCS Worldwide Military Command and Control System

Multilevel Security is NOT the Same as Information Security!

The DOD Multilevel Security Office does not have the final word on computer or network security. We do, however, rely on a number of security experts as we implement MLS solutions. Our goal is to meet operational requirements while managing the associated security risks created by linking systems together. Sometimes we have had to tell our customers that the technology simply isn't available (at their level of cost) to do what they want to do.

Even More Important!

An A1-evaluated computer system is not infallible. A malicious program can crash a "secure" system. To quote from Firewalls and Internet Security: Repelling the Wily Hacker, by William R. Cheswick and Steven M. Bellovin (Addison-Wesley, 1994):

In the case of the [Internet] Worm, for example, most of the structural safeguards of the Orange Book would have done no good at all. At most, a high-rated system would have confined the breach to a single security level. But effectively, the Worm was a denial-of-service attack, and it matters little if a multilevel secure computer is brought to its knees by an unclassified process or by a top secret process. Either way, the system would be useless.